PRÉSE
NOTRE
HOMOLOGATION

QUENTIN POIDEVIN, FLORIAN MORA, ROBIN FOUGERON, RANIA ARAR

SOMMAIRE

I. PRÉSENTATION DU SI DE XSPACE

XSPACE

D'USAGE

Mission de l’organisation :

- Xspace est une PME française spécialisée dans le développement de solutions technologiques innovantes. La société a été sélectionnée par le Ministère de la Défense tchèque pour réaliser un projet classifié RUE impliquant l’échange et la production d’informations sensibles dans un cadre de défense.

Contexte d’usage :

- Le SI est dédié à 10 personnes habilitées.
- L’usage se fait en salle sécurisée (KANAL) et lors de déplacements.
- L’architecture est isolée et renforcé, sans accès Internet, avec mises à jour via station blanche.
- Le matériel et la cryptographie utilisés sont qualifiés UE .
- L’objectif est de garantir confidentialité, intégrité, disponibilité et traçabilité des données classifiées.

Enjeu immédiat :

- **L’homologation est requise dès maintenant afin de débuter la mission avec l’État tchèque dans un cadre conforme aux exigences RUE.**

I.2 PÉRIMÈTRE D'HOMOLOGATION

Périmètre fonctionnel

Le périmètre couvre l'ensemble des activités liées au contrat RUE :

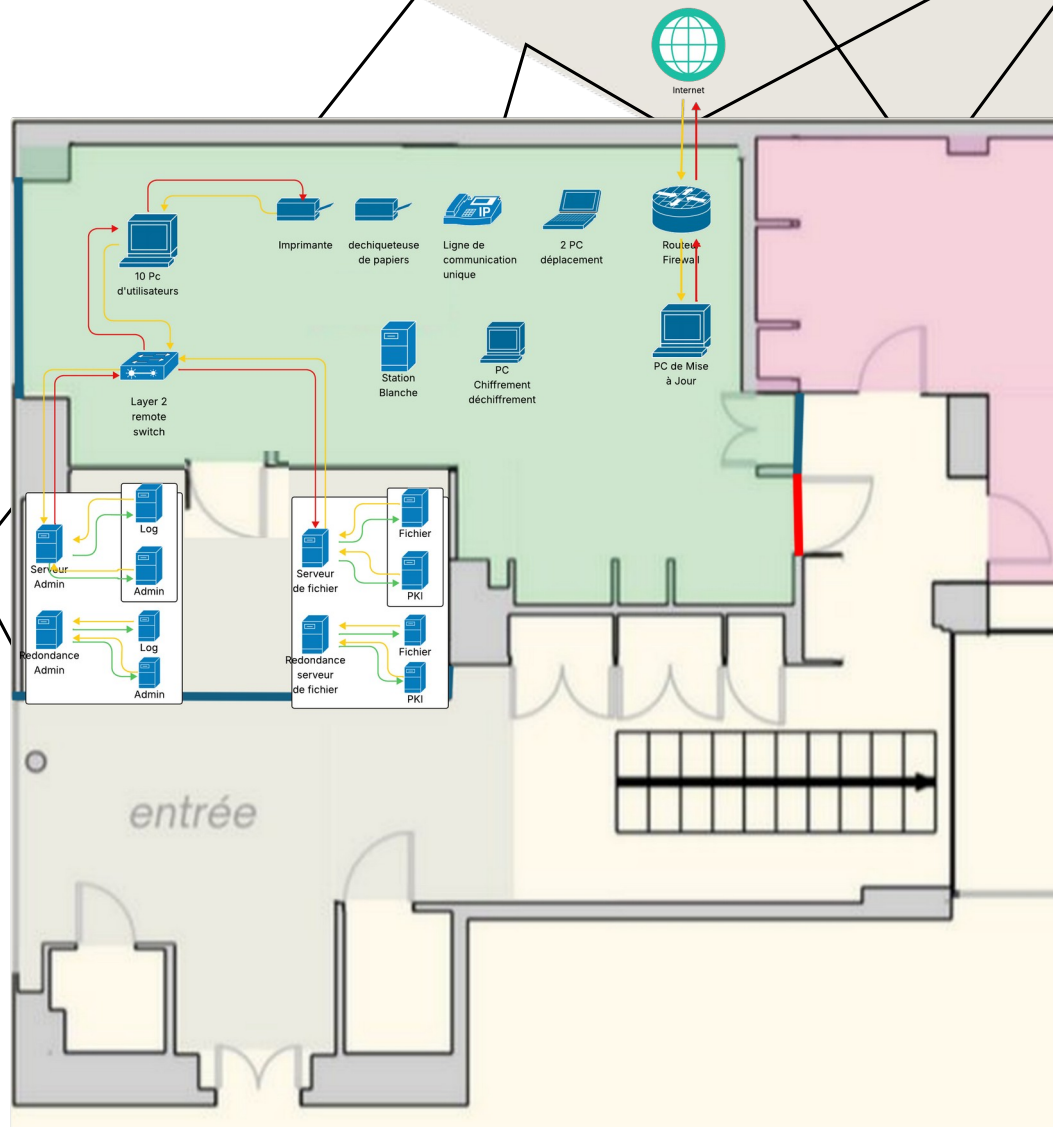
- production et consultation de documents classifiés,
- stockage interne des données,
- échanges sécurisés avec le Ministère de la Défense tchèque,
- gestion des identités et habilitations,
- traçabilité des opérations.

Périmètre technique

L'étude porte sur le SI dédié à la gestion et au traitement d'informations classifiées RUE, hébergé dans les locaux Xspace, sans interconnexion Internet directe.

Éléments inclus :

- 10 PC utilisateurs dédiés au contrat, interconnecté
- 2 PC de déplacement (durcissement renforcé)
- VLAN utilisateurs séparés, switch L2 isolé
- Services centralisés internes :
  - § AD-Admin, AD-Log
  - § Serveur de fichiers / VM Files
  - § PKI interne pour la gestion des clés
  - § Serveur de redondance
- PC de mise à jour isolé
- Pc de chiffrement / déchiffrement isolé
- Station blanche d'analyse amont USB
- Routeur/Firewall (hors Internet sauf usage « mise à jour »)
- Local serveur sécurisé
- Salle Kanal (traitement classifié et renforcé voir DAT)



Exclusions

Seuls les éléments manipulant ou stockant de l'information classifiée sont intégrés afin de garantir un contrôle complet et une homologation ciblée.

Hors périmètre :

- SI classique non classifié de l'entreprise (pour réduire le périmètre et éviter les connexions non maîtrisées)
- systèmes personnels, BYOD
- accès Internet utilisateurs (incompatible exigences RUE)
- Service de surveillance (Caméras)

I.3 ENJEUX DE SÉCURITÉ

Protection de l’information
•Accès strictement réservé aux personnes habilitées
•Prévention des fuites, copies ou divulgations, y compris lors des déplacements ou via supports amovibles

Intégrité des documents
•Documents et livrables exacts, non modifiés et identifiables
•Détection rapide des modifications non autorisées

Confidentialité et cryptographie
•Cycle de vie des clés sécurisé : génération, stockage, usage, révocation
•Signature et chiffrement conformes aux standards européens (UE)

Disponibilité des ressources critiques
•Serveurs, postes et espaces de travail toujours opérationnels
•Plans de sauvegarde et reprise adaptés pour assurer continuité même en mode dégradé

Traçabilité et audit
•Enregistrement fiable et horodaté de toutes les actions
•Analyse des incidents et preuve non-répudiable

Sécurité hors connexion
•Mises à jour et transferts via stations blanches pour éviter le code malveillant
•Contrôle strict des flux physiques (USB, disques, documents

Postes en mobilité
•Chiffrement complet et authentification forte
•Protection physique contre perte ou vol

Simplicité et maîtrise de l’architecture
•Architecture isolée et segmentée, sans accès Internet
•Réduction des surfaces d’attaque et maîtrise opérationnelle facilitée

Conformité RUE
•Respect des exigences européennes : cryptographie qualifiée UE, contrôle des accès, cloisonnement réseau, sécurisation des locaux
•Procédures opérationnelles adaptées

Maîtrise des risques internes
•Limitation des erreurs humaines et risques d’insider
•Droits et accès strictement contrôlés

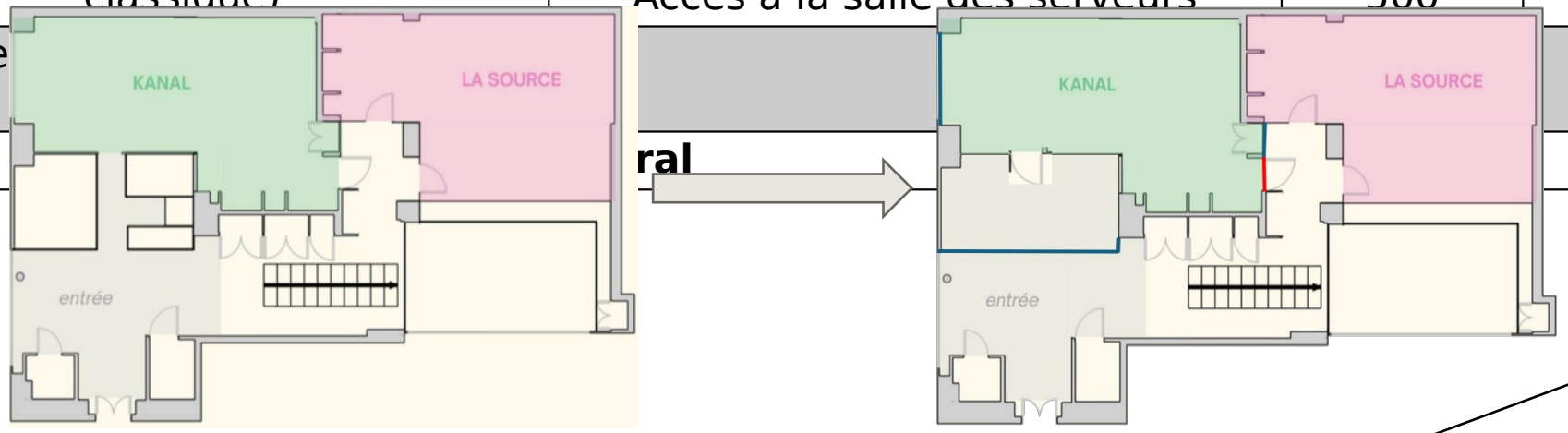
Confiance du partenaire
•Sécurité conforme aux standards RUE
•Garantir crédibilité et démarrage rapide du projet après homologation

***Standards RUE :** ensemble de règles européennes pour protéger les informations classifiées, incluant cryptographie qualifiée, contrôle des accès, cloisonnement réseau et sécurisation des locaux.

II. TRAVAUX MENÉS POUR L'HOMOLOGATION

II.1 HISTORIQUE DES TRAVAUX PHYSIQUES

Budget total estimatif			
Poste	**Commentaire**	**Coût min (€)**	**Coût max (€)**
Sol blindé			
Fenêtre P6B + panneau opaque + cadre	Conformité RUE et SPID-29/30	5120	6620
Mur composite blindé	Conformité RUE et SPID-29/30	4000	4500
Ossature / renfort structure		1500	2000
Porte métallique blindée simple	Conformité RUE et compatible SPID-29/30	2500	4000
Portique métal simple (détecteur classique)	Accès à la salle des serveurs	500	1500
Ajuste			4000
	ral		**22620**



II.2 HISTORIQUE DU MATÉRIEL

Equipement	Quantité	Commentaire
Ordinateur employé	12	10 employés + 2 en stock – Ordinateur reconditionné sans disque dur
Ordinateur mise à jour	1	Ordinateur reconditionné sans disque dur
Ordinateur chiffrement / déchiffrement	1	Ordinateur reconditionné sans disque dur
Câble antivol	14	
Câble HDMI blindé	14	braided and foil shielding
Câble RJ 45 blindé	18	S/FTP
Verrou rj45	20	
Verrou USB	200	
Ecran PC	14	
Câble d'alimentation écran	14	
SSD 256Go Samsung PM9B1 NVMe M.2 PCIe	14	SSD vierge afin de remplacer ceux des PC reconditionnés
PC de transport	2	PC portable pour déplacement pro (à durcir)
Serveurs (fichier, administration et redondance)	4	Homologué ANSSI
Pare-feu+ licence (stormshield)	1	Homologué ANSSI
1 switch (cisco)	1	Homologué ANSSI
Ligne de téléphone unique (cuivre)	1	Sans wifi/bluetooth
Imprimante	1	Sans wifi/bluetooth
Destructeur de fichier (P-7)	1	Plus haute sécurisation, norme DIN 66399
Clé usb Kingstone	2	Avec clavier
Yubikey	13	Une par employé, une pour l'administrateur et 2 en stock
Station blanche	1	
Lecteur de bande LTO	1	
Bandes LTO	15	10 pour la rotation + 5 en stock

II.3 BUDGET TOTAL

Budget total estimatif		
Périmètre	**Coût min (€)**	**Coût max (€)**
Travaux physique	16 170 €	22 620 €
Matériel	25 322 €	25 322 €
Total général	41 492 €	47 942 €

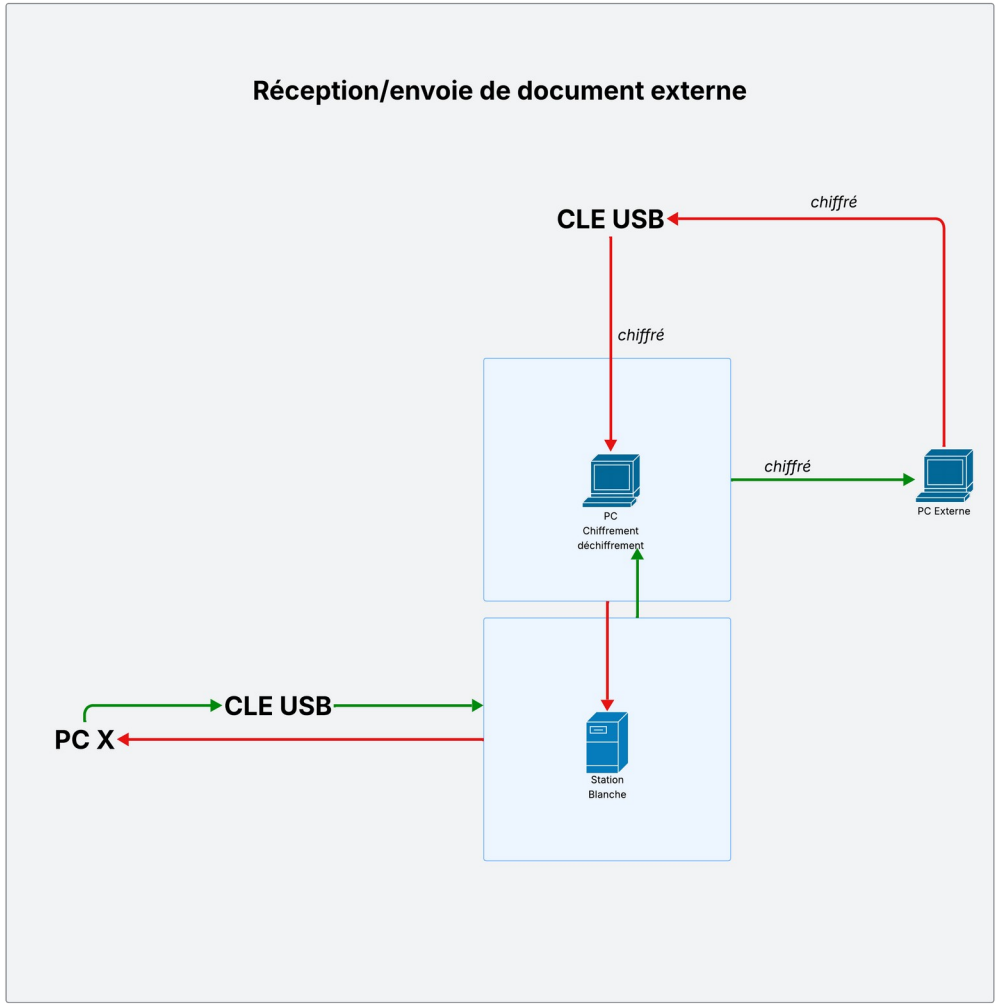
III. SOCLE DE SÉCURITÉ

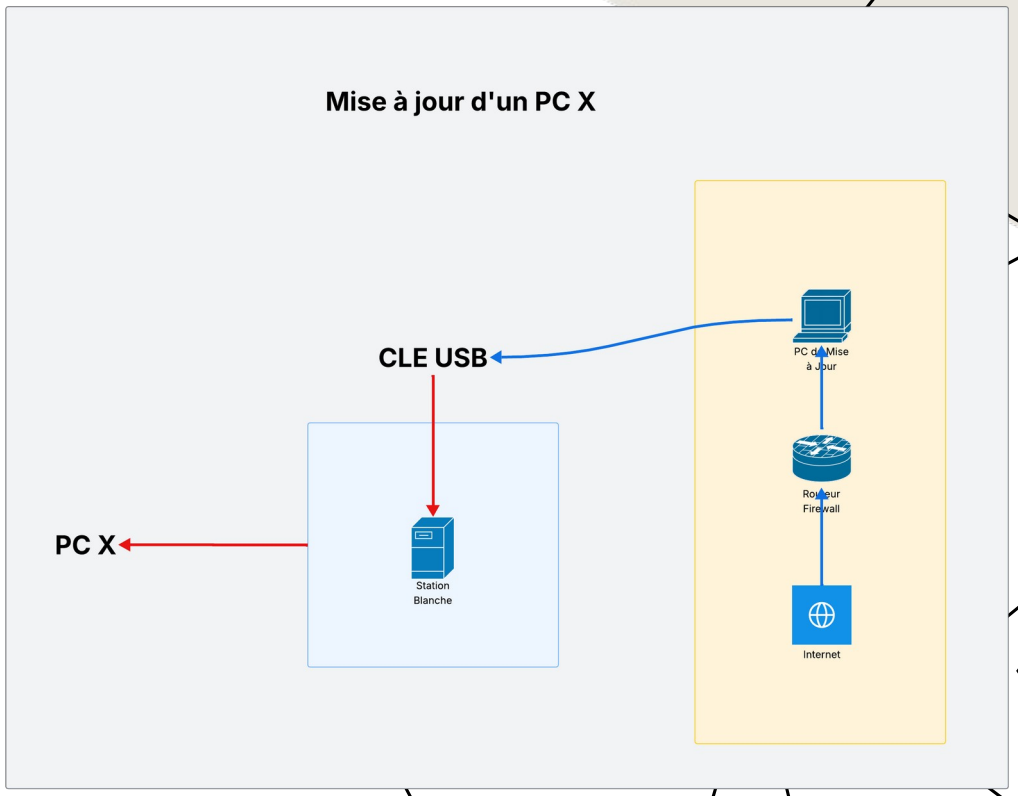
III. SOCLE DE SÉCURITÉ (1,2,3,4)

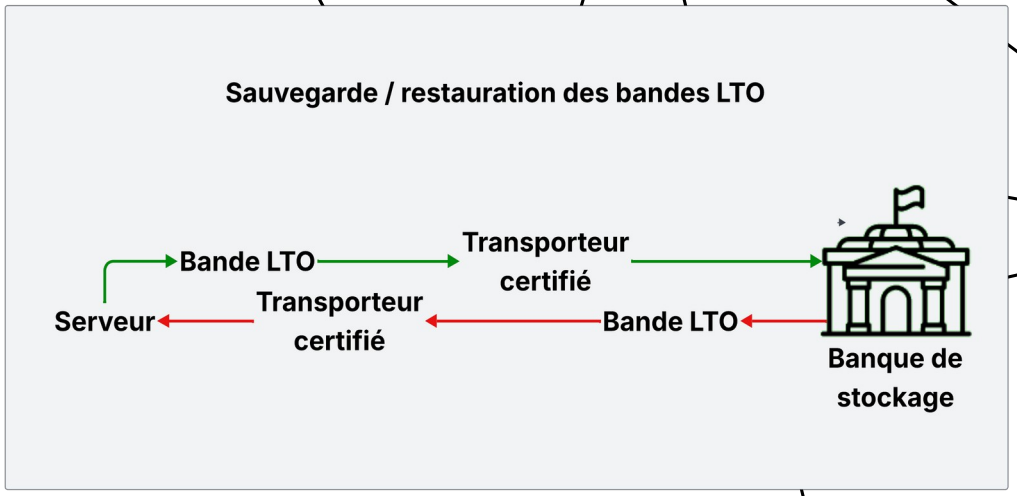
Thématique	Référentiel / Politique de Sécurité	État d'Application	Écart Constaté (Faiblesse)	Justification / Mesures Compensatoires
1. Réglementaire & Physique	**IGI 1300 / II 901** *(Protection du secret de la défense nationale)*	**Partiel**	La salle "KANAL" est renforcée mais ne dispose pas d'une certification "Zone Protégée" (coût infrastructure > budget).	**Compensation Organisationnelle :** ▪ Contrôle d'accès strict (Badge + Code) ▪ Registre papier des entrées/sorties. ▪ Interdiction formelle des smartphones en salle (Casiers à l'entrée).
2. Gestion des Supports (USB)	**PSSI – Politique de Gestion des Supports Amovibles** *(Réf : Note ANSSI Station Blanche)*	**Partiel**	Le transfert de données (Mises à jour/Livrables) repose entièrement sur des clés USB, vecteur d'attaque majeur pour les réseaux isolés (Air-Gap).	**Mesure Technique & Procédurale :** ▪ Usage obligatoire de la Station Blanche pour décontamination (scan antivirus) avant toute connexion au réseau. ▪ Ports USB des PC utilisateurs bloqués physiquement ou logiquement (sauf clavier/souris). ▪ Utilisation exclusive de clés USB identifiées et chiffrées par l'entreprise.
3. Nomadisme (Missions)	**Guide ANSSI "Partir en mission" / PSSI Nomadisme**	**Non Appliqué**	Les 10 collaborateurs partent en République Tchèque avec des "PC Mission" contenant des données sensibles, sans procédure de retour stricte.	**Mesure Technique :** ▪ Configuration stricte des ACLs (Access Control Lists) sur le switch.D2:D42 ▪ Administration des serveurs uniquement depuis la VM dédiée "Service Admin" (saut de bastion)
4. Authentification & Crypto	**RGS (Référentiel Général de Sécurité) / Qualifié UE**	**Appliqué**	Les mots de passe seuls sont insuffisants pour l'accès aux données RUE.	**Mesure Technique :** ▪ Authentification à double facteur (MFA) via clé matérielle (ex: YubiKey/Token qualifié ANSSI/UE) pour l'ouverture de session. ▪ Certificats stockés sur carte à puce/token, pas sur le disque.
5. Cloisonnement Réseau	**Architecture de Défense en Profondeur** *(Ségrégation Admin/Utilisateur)*	**Partiel**	L'architecture repose sur des VLANs (Admin / Utilisateur / Serveur) sur un même commutateur (Switch) physique, faute de budget pour des équipements séparés.	**Mesure Technique :** ▪ Configuration stricte des ACLs (Access Control Lists) sur le switch. ▪ Administration des serveurs uniquement depuis la VM dédiée "Service Admin" (saut de bastion)
6. Maintien en Condition de Sécurité	**Guide d'Hygiène Informatique (ANSSI)** *(Gestion des mises à jour)*	**Appliqué**	Absence de connexion Internet directe pour les mises à jour (Windows/Antivirus). Le parc risque de devenir obsolète rapidement.	**Mesure Procédurale :** ▪ Processus mensuel : Téléchargement des patchs sur PC Internet (Zone Jaune) -> Scan Station Blanche -> Import sur Serveur WSUS interne.
7. Gestion des Incidents	**Procédure de Réaction aux Incidents**	**Non Appliqué**	Aucune chaîne d'alerte définie en cas de perte de PC en mission ou de détection de virus sur une clé USB.	**Mesure Organisationnelle :** ▪ Nomination d'un référent sécurité joignable 24/7. ▪ Fiche réflexe "Perte de matériel" distribuée aux voyageurs (qui appeler, que déclarer).

IV. ANALYSE DE RISQUE

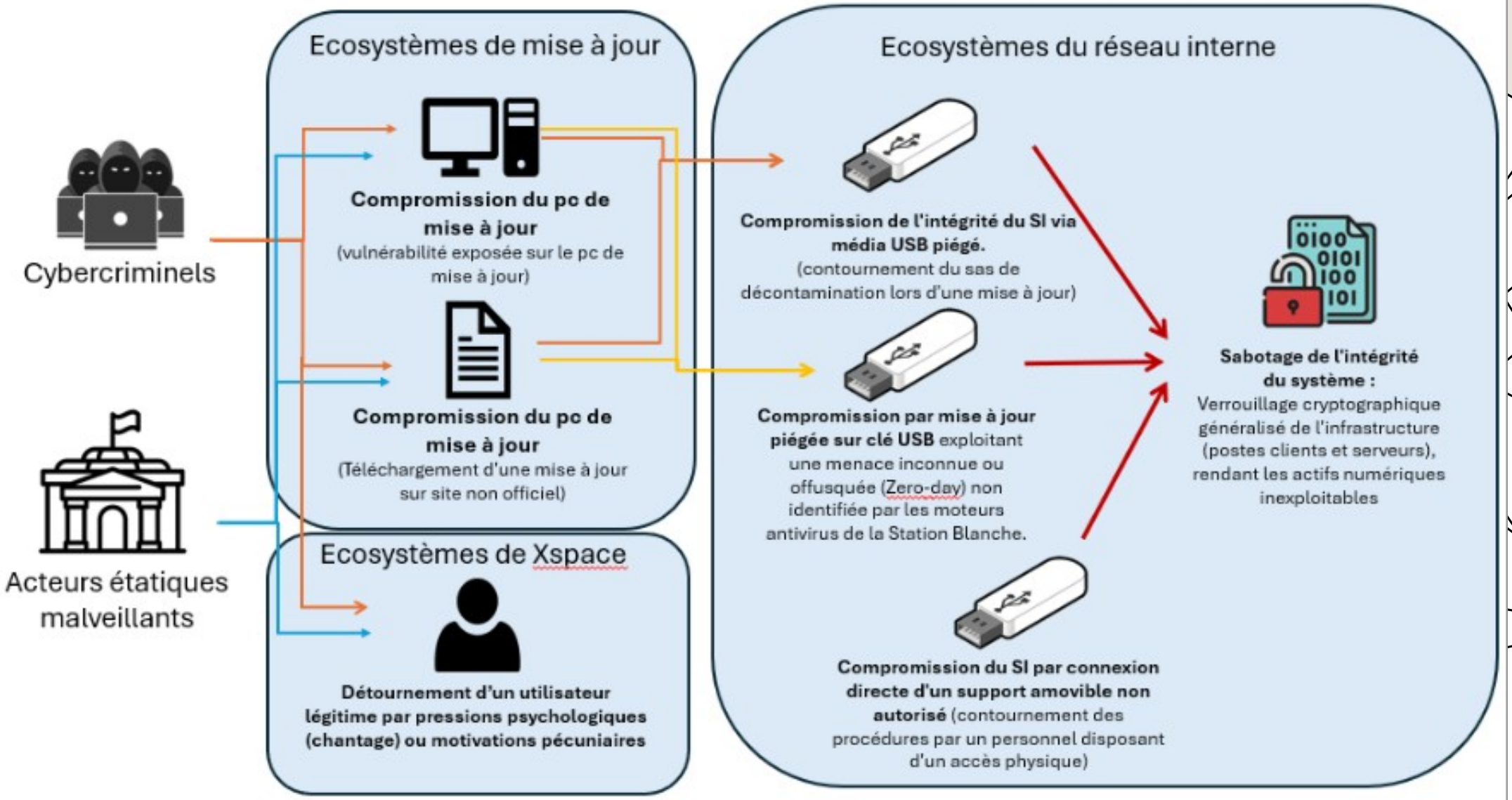
IV.1 FLUX CLASSIQUE



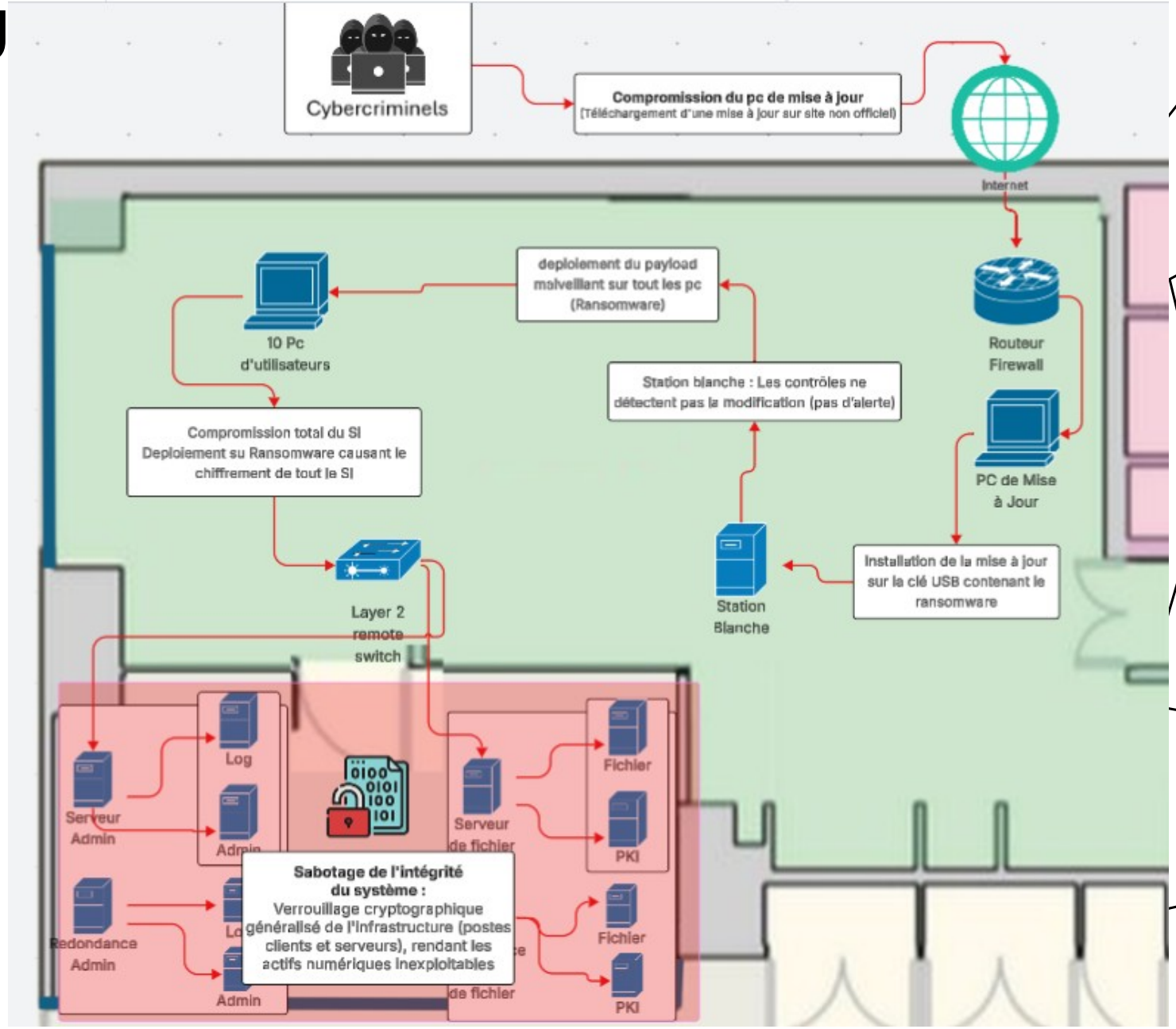




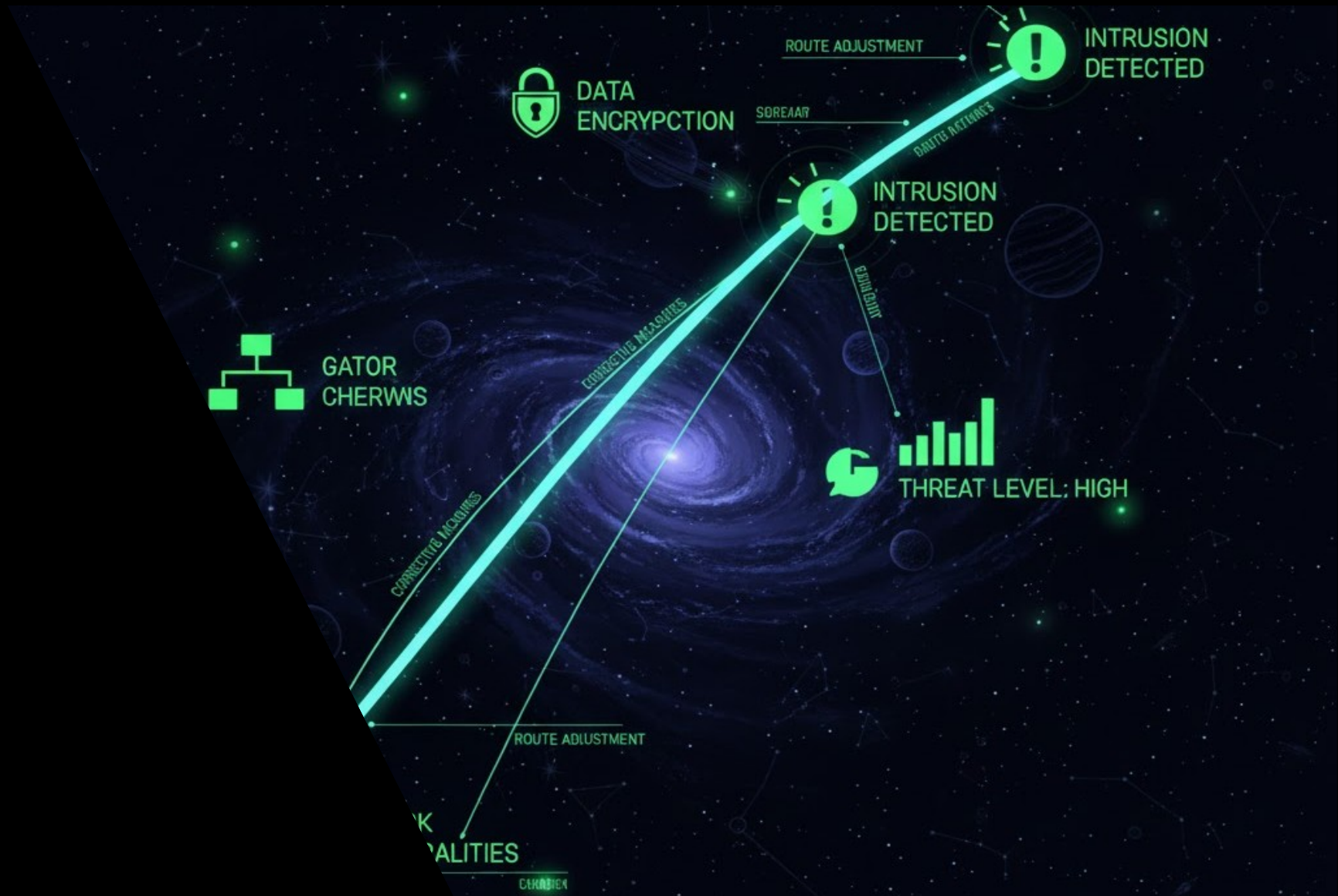
IV.2 SCÉNARIOS D'ATTAQUE CRITIQUES



IV.3 SCÉNARIOS D'ATTAQUE CRITIQU



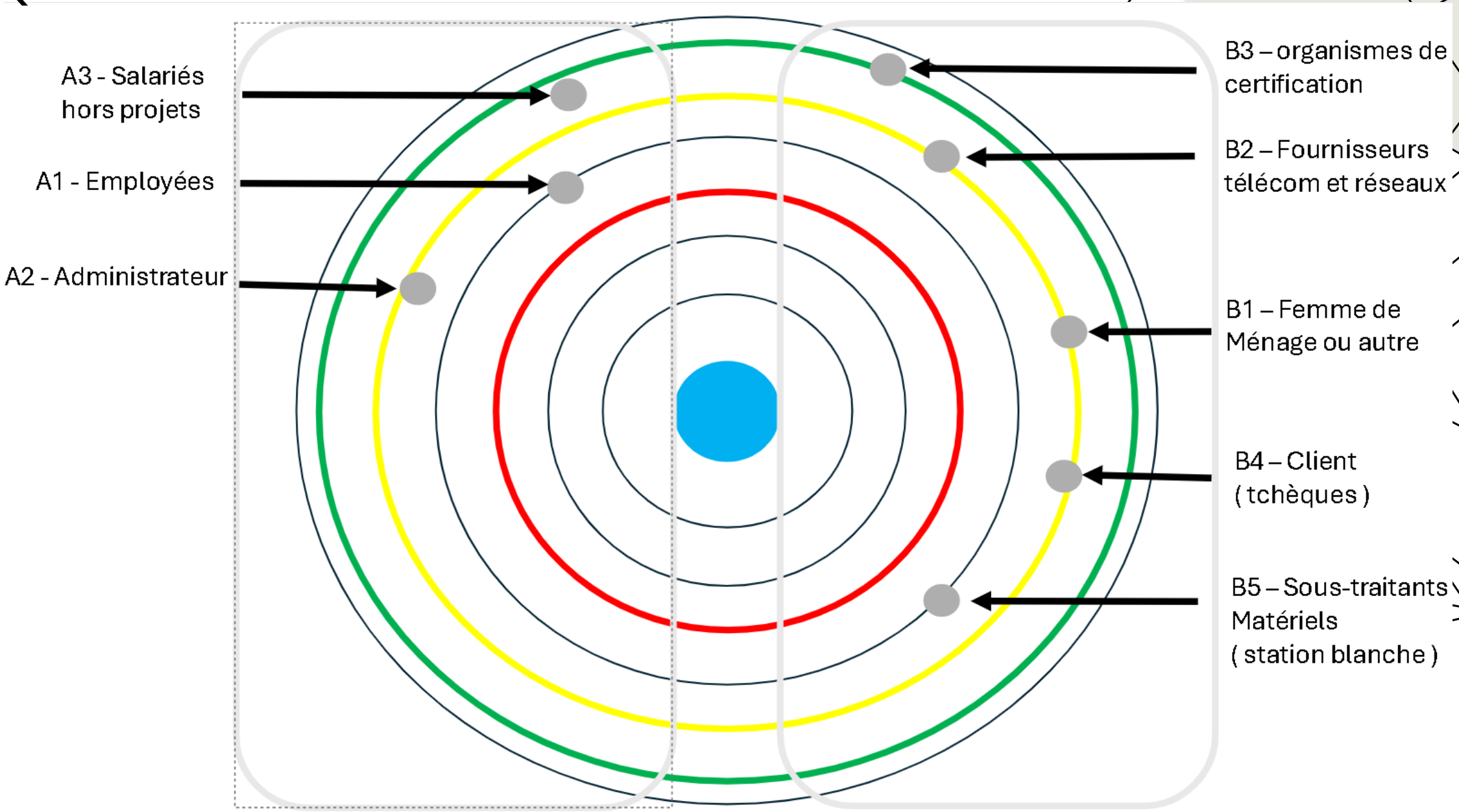
V. PLAN DE TRAITEMENT DES RISQUES



V.1 MESURES DE TRAITEMENT DES RISQUES

ID	PARTIE PRENANTE	CHEMINS D'ATTAQUE	STRATÉGIQUES	MESURES DE SÉCURITÉ	GRAVITE	VRAISEMBLANCE	MENACE INITIALE	MENACE RÉSIDUELLE
R27	Administrateur / opérateur mise à jour	Diffusion involontaire d'une mise à jour compromise ou non sécurisée	Introduction d'un ransomware par mise à jour (involontaire)	Validation automatisée des mises à jour (hash, signature, provenance), station blanche avec sandbox, workflow 4-eyes, monitoring post-déploiement, logs immuables, plan de restauration testé	4	3	3,5	1,3
R28	Prestataire nettoyage (accès opportuniste)	Branche une clé USB si accès ouvert par erreur	Infection par clé USB lors d'un accès furtif	Interdiction totale du nettoyage pendant les heures d'accès, **badge blacklisté sur la salle, sas sécurisé, fermeture automatique des portes, capteurs d'ouverture + alarme immédiate, cache-ports physiquement verrouillés, screensaver instantané + cable lock, patrouilles SSI, traitement des rebuts (aucun poste laissé alimenté)**	4	3	3,5	0,5
R29	Employé mécontent (accès local autorisé)	Branche une clé USB personnelle sur un poste isolé	Infection par malware/ransomware pour bloquer la production	**Blocage matériel des ports USB, station blanche dédiée aux supports, poste scellé (tamper-evident), accès sous supervision (caméra + 4-eyes), audits d'intégrité du BIOS/UEFI, traçabilité forte des actions, suppression des privilèges locaux, contrôle comportemental EDR offline, politique disciplinaire appliquée**	**4**	**3**	3,5	0,5

V.1 MESURES DE TRAITEMENT DES RISQUES



V.1 MESURES DE TRAITEMENT DES RISQUES

Gravité					
	4 – Critique	R3 – R22 R27 – R28 - R29	R1 – R4 – R7 - R25		
	3 - importance	R2 – R6 – R11 – R14 – R20 – R21	R5 – R9 – R10 – R19 – R23 – R24 - R26		
	2 - Significatif	R8 – R13 – R15 – R17 - R18	R16		
	1 - Faible		R12		
		1 – Peu probable	2 - probable	3 - Très probable	4 - Quasi certain
		Vraisemblance			

V.2 RISQUES RÉSIDUELS

Gravité					
	4 - Critique	R3 - R22	R1 – R4 – R7 - R25	R27 – R28 - R29	
	3 - importance	R2 – R6 – R11 – R14 – R20 – R21	R5 – R9 – R10 – R19 – R23 – R24 - R26		
	2 - Significatif	R8 – R13 – R15 – R17 - R18	R16		
	1 - Faible		R12		
		1 – Peu probable	2 - probable	3 - Très probable	4 - Quasi certain
		Vraisemblance			

Gravité					
	4 – Critique	R3 – R22 R27 – R28 - R29	R1 – R4 – R7 - R25		
	3 - importance	R2 – R6 – R11 – R14 – R20 – R21	R5 – R9 – R10 – R19 – R23 – R24 - R26		
	2 - Significatif	R8 – R13 – R15 – R17 - R18	R16		
	1 - Faible		R12		
		1 – Peu probable	2 - probable	3 - Très probable	4 - Quasi certain
		Vraisemblance			

V.2 RISQUES RÉSIDUELS

- R27 – Administrateur / opérateur mise à jour

Diffusion involontaire d'une mise à jour compromise

Introduction d'un ransomware par mise à jour

Résiduel : Malgré les mesures de sécurité renforcées, le risque de diffusion involontaire d'une mise à jour compromise par un administrateur reste **faible en probabilité**, grâce au contrôle strict de la chaîne de mise à jour.

- R28 – Prestataire nettoyage

Branche une clé USB

Infection par clé USB

Résiduel : L'introduction d'un malware par clé USB lors d'un accès furtif d'un prestataire de nettoyage devient **très improbable** grâce à un ensemble de mesures combinées

L'acteur opportuniste ne dispose plus **ni du temps**, **ni de l'accès**, **ni de la surface technique** nécessaires pour exploiter la vulnérabilité initiale.

- R29 - Employé mécontent - Branche une clé USB personnelle – infection par malware

Résiduel : Grâce au blocage matériel des ports USB, aux scellés tamper-evident, à la supervision systématique (caméra + double-contrôle), à l'absence de privilèges locaux, à la station blanche obligatoire et à l'EDR comportemental, la possibilité pour un employé mécontent d'introduire volontairement un malware via une clé USB sur un poste isolé devient **extrêmement improbable**.

VI. PROPOSITION D'AVIS

VI. PROPOSITION D'AVIS

- **Sécurité globale :**

Le système d’information de Xspace protège efficacement les informations classifiées, grâce à la mise en place de mesures robustes.

- **Mesures conformes aux standards RUE :**

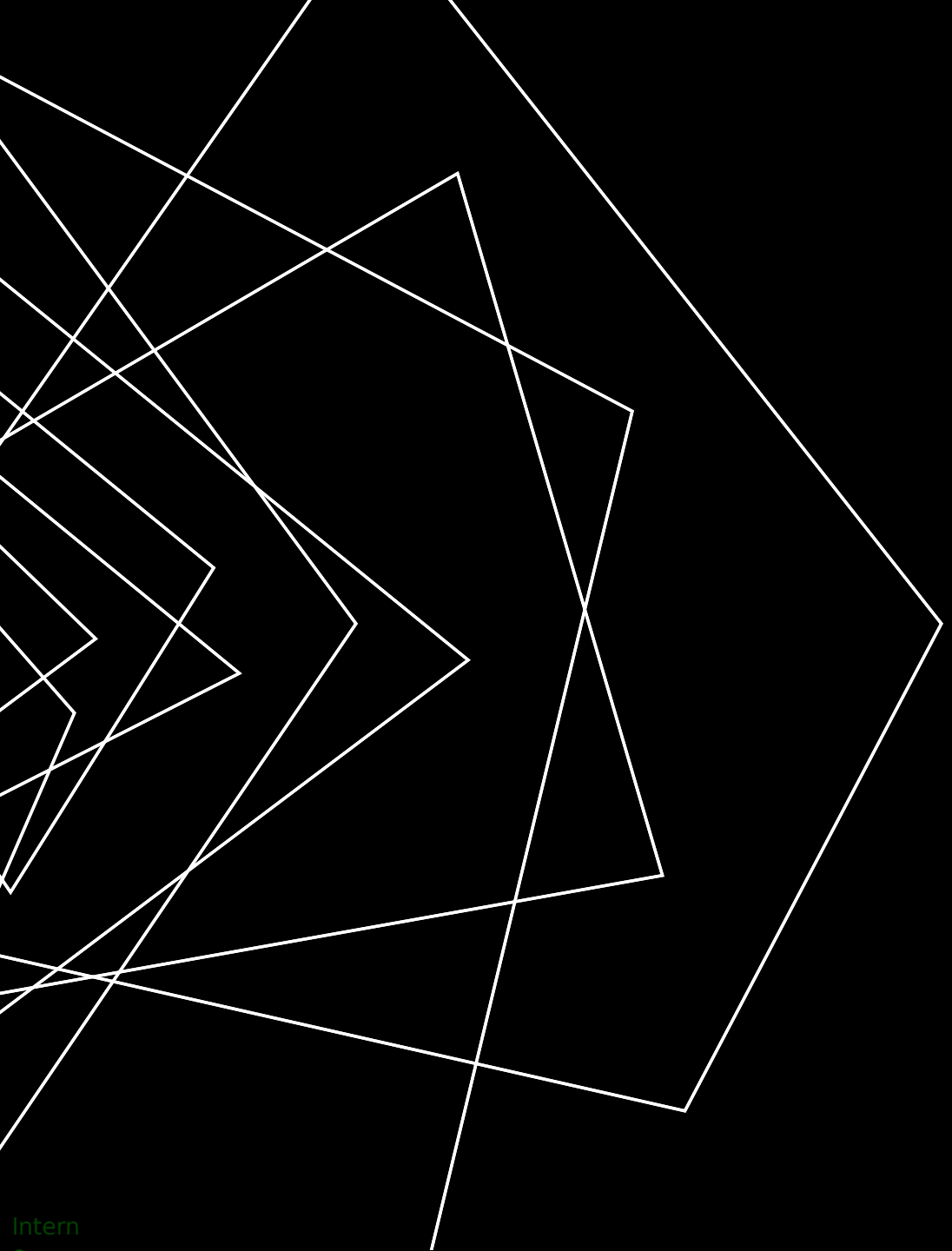
Cryptographie qualifiée, postes durcis avec protection contre le vol et la perte, traçabilité complète des actions, architecture réseau isolée et segmentée.

- **Risques résiduels :**

Quelques risques subsistent, notamment sur les postes mobiles en déplacement, mais ils sont faibles et bien maîtrisés grâce aux procédures de sécurité et de surveillance.

- **Recommandation finale :**

L’homologation du SI peut être accordée. Il est recommandé de maintenir un suivi régulier et de renforcer la sécurité des postes mobiles pour garantir la continuité de la protection.



MERCI

QUENTIN POIDEVIN
FLORIAN MORA
ROBIN FOUGERON
RANIA ARAR

Intern